# Open Horizon project
# TSC Meeting

May 23, 2022


THE LINUX FOUNDATION

LF EDGE

# Meeting Details

Time: May 23, 2022 11:00 AM Pacific Time (US and Canada)

Please download and import the following iCalendar (.ics) files to your calendar system.
https://zoom.us/meeting/tJMrce2hqTIjHNa60DHyv9sn847QK4LGK_Gf/ics?icsToken=98tyKuCvqD0uE9OcuR-FRowEBI_oLPPwtlhEgo1cyk_BKzlFOxD4brYVA5krPP_7

Join Zoom Meeting
https://zoom.us/j/97664979962?pwd=TlY3dUk4K0Y3WnZXMjVMeisreGRkQT09

Meeting ID: 976 6497 9962
Passcode: 312515

Find your local number: https://zoom.us/u/ac5YZ6pqGW

# LF Antitrust Policy Notice

Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

# Open Horizon TSC

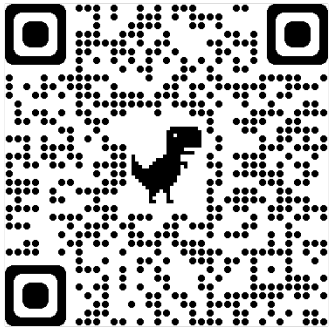
| Working Group or Partner | Representative |
|---|---|
| Agent | David Booz |
| DevOps | Ben Courliss |
| Documentation | Joe Pearson |
| Examples | Troy Fine |
| Management Hub | Nathan Phelps |
| Outreach | Susan Bowlin |
| Partner: mimik Technology | Michel Burger |
| Partner: IBM | Kavitha Bade |

# Announcements

THE LINUX FOUNDATION
LF EDGE

# Spring 2022 Mentorship wrapping up

- See the LFX Mentorship schedule
  - Final mentee evaluations due next week
  - Mentee feedback and/or blog submissions due
  - Second stipend request submitted on 31st and after evaluations
- Glen Darling is presenting to RCOS summer session
- Joe is fundraising for stipends for future LFX mentorships
  - Pass the word, donations accepted here



# What is an SBOM?

“SBOMs are a cornerstone of software supply-chain security.” - various

From the NTIA: “A ‘Software Bill of Materials’ (SBOM) is a nested inventory for software, a list of ingredients that make up software components and provides vital information about the components themselves.”

The Cybersecurity & Infrastructure Security Agency (CISA) states: “A ‘software bill of materials’ (SBOM) has emerged as a key building block in software security and software supply chain risk management. The SBOM work has advanced since 2018 as a collaborative community effort, driven by NTIA’s multistakeholder process. ”

Linux Foundation Webinar: The role of SBOM in cybersecurity readiness.

# What problems does it solve?

- Identity: Executing the intended application
- Provenance: Knowing the vendor, license, version, dependencies
- Tamper-evident: Matching component signature and certificate
- Compliance: Meeting regulations and standards (EO, ISO, GDPR, FAR)

# Where should it be used?

- To scan Open Horizon source code in each repository
- When building and publishing code artifacts (packages, containers)
- When running Open Horizon
- When publishing service definition files and policies with OH
- When managing container lifecycles with OH
- When OH forms agreements (policies based on SBOM properties)
- When OH is initially installed, including zero-touch scenarios

# How to generate an SBOM for an OH component

| | |
|---|---|
| Install syft on macOS | `brew update; brew tap anchore/syft; brew install syft` |
| Scan anax container | `syft openhorizon/amd64_anax` |
| SBOM from container | `syft openhorizon/amd64_anax:latest -o syft-json=sbom.anax.json` |
| SBOM from GH clone | `syft packages dir:dev/anax -o syft-json=sbom.anax-source.json` |
| Display SBOM abbv. | ✓ Loaded image<br>✓ Parsed image<br>✓ Cataloged packages [283 packages]<br><br>NAME VERSION TYPE<br>acl 2.2.53-1.el8 rpm<br>audit-libs 3.0-0.17.20191104git1c2f876.el8 rpm<br>basesystem 11-5.el8 rpm<br>bash 4.4.20-1.el8_4 rpm<br>brotli 1.0.6-3.el8 rpm<br>bzip2-libs 1.0.6-26.el8 rpm<br>ca-certificates 2020.2.41-80.0.el8_2 rpm<br>chkconfig 1.13-2.el8 rpm<br>coreutils-single 8.30-8.el8 rpm<br>cracklib 2.9.6-15.el8 rpm<br>cracklib-dicts 2.9.6-15.el8 rpm<br>crypto-policies 20210209-1.gitbfb6bed.el8_3 rpm<br>crypto-policies-scripts 20210209-1.gitbfb6bed.el8_3 rpm<br>cryptsetup-libs 2.3.3-4.el8 rpm<br>curl 7.61.1-18.el8 rpm |
| Generate attestation | See syft README.md for instructions on how to generate attestation with local private key and upload to OCI registry |

# Working Group Updates

THE LINUX FOUNDATION
LF EDGE

# Next Meeting

THE LINUX FOUNDATION
LF EDGE

# Next Meeting

- Next Meeting: Monday, June 6 @ 11:00am PT/02:00pm ET

# Thank You

THE LINUX FOUNDATION
LF EDGE

# Repositories per Working Group

| Agent | DevOps | Documentation | Examples | Mgmt Hub |
|---|---|---|---|---|
| anax<br>edge-sync-service<br>edgeengine-integration<br>edge-sync-service-client<br>rsapss-tool<br>mms-cloud-container | devops<br>horizon-deb-packager<br>edge-utilities | .github<br>artwork<br>open-horizon.github.io<br>documentation-migration<br>project-summary | examples<br>open-horizon-services | exchange-api<br>SDO-support<br>vault-exchange-auth |